Project 5:Disaster recovery with IBM

cloud virtual server

Project Title: Disaster recovery

Name : Poojasree
Register Number : 411521104082

Configuration replication:

. Avoid split-brain situation Keep in mind that only one cluster behaves as a primary. ...

- Enable DR primary replication Enable DR replication on the primary cluster (Cluster A). ...
- Enable DR secondary replication ...
- DR operation token strategy ...
- Promote DR secondary to primary …

Disaster recovery testing

- Last updated 2023-07-31

Disaster recovery (DR) testing is what you must do to keep your ability to be resilient, hoping not to need to do it for real. There are different types of disaster recovery testing that you can do to verify your resiliency capabilities:

- DR dry test
- DR simulation
- Switch-over

Disaster recovery dry test

A DR dry test is performed by checking all of the resource availability and runbooks on paper, without running a real DR simulation or switch-over.

This type of testing is normally run with higher frequency compared to the other testing flavors as no real activities are performed, but it does require the same effort in terms of skills and people.

Disaster recovery simulation

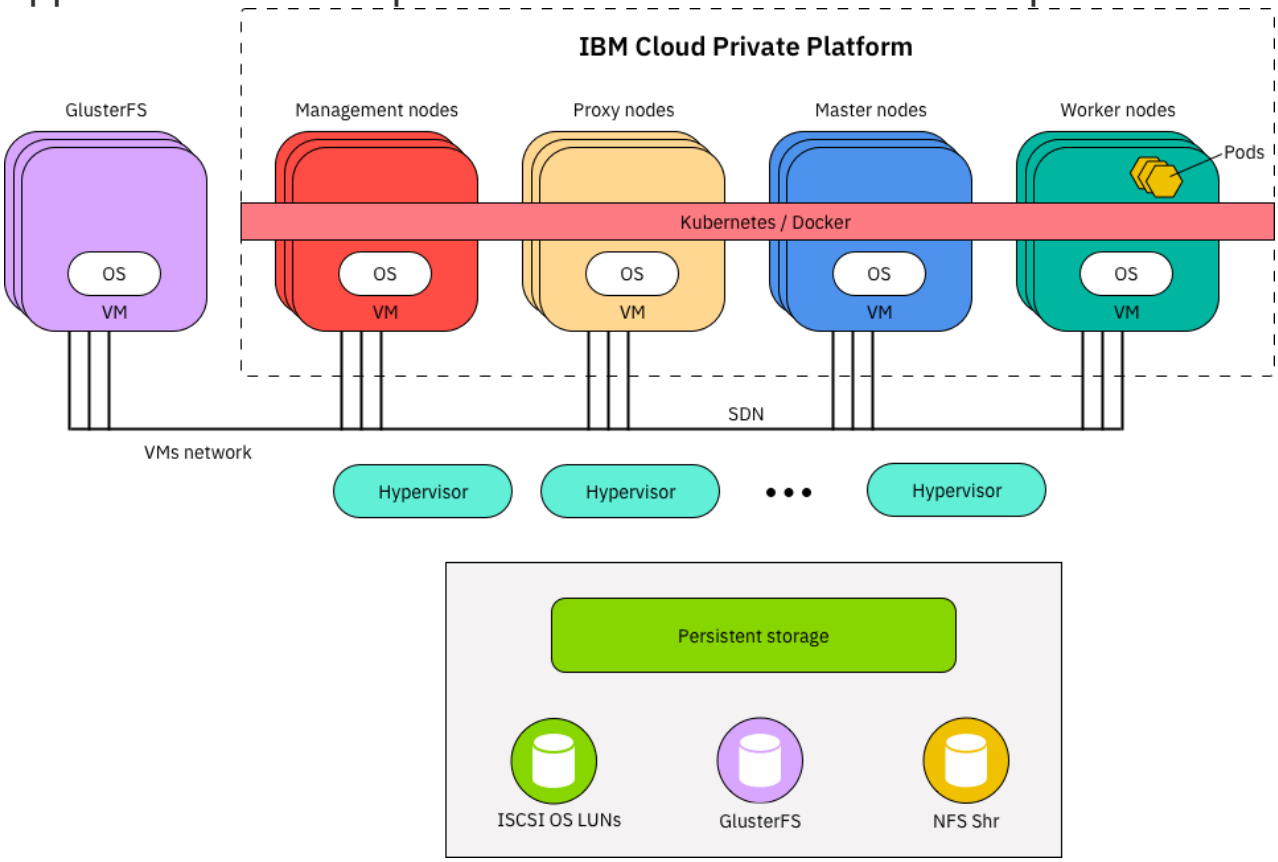
DR simulation is a way to verify or audit the emergency runbooks and check the recovery time objectives (RTO) and recovery point objectives (RPO) provided by the solution by simulating as much as possible in the same conditions as a real emergency.

Switch-over

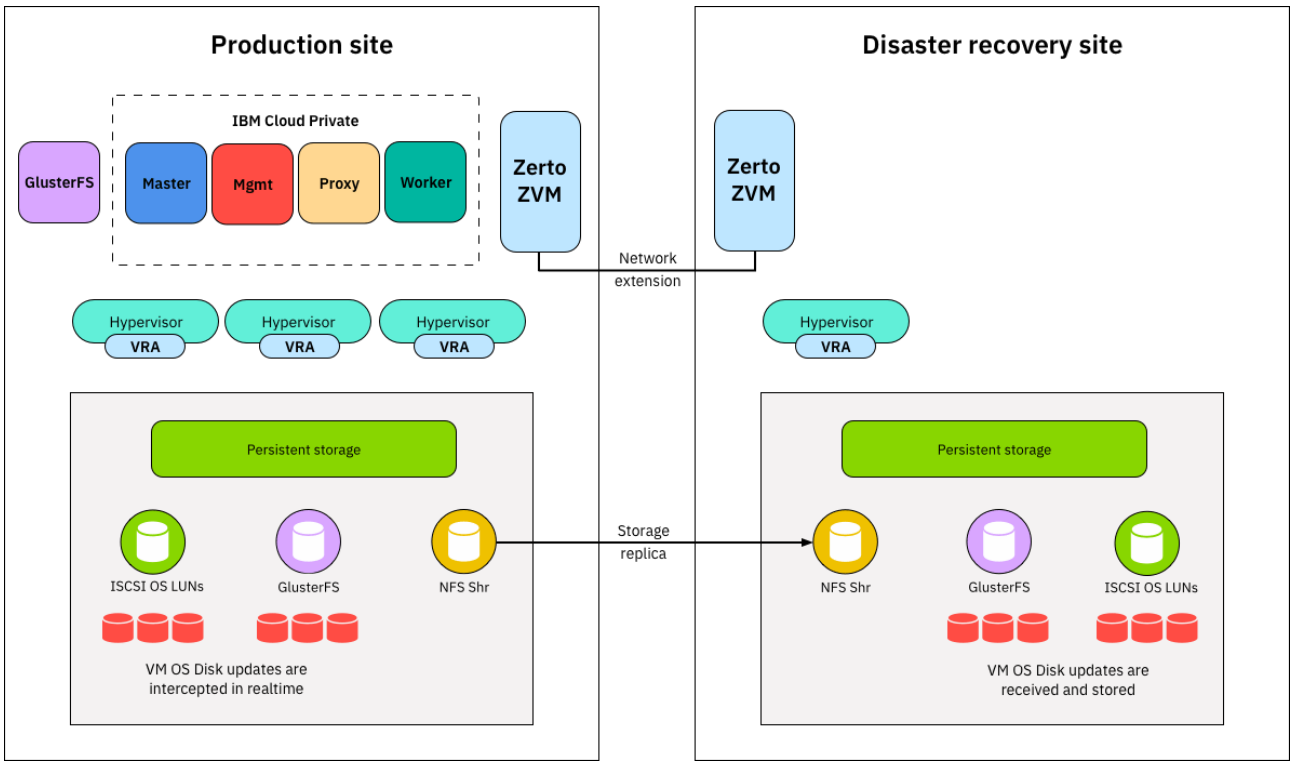
Opposite to the DR simulation, in the switch-over test, production is moved from primary site to DR site to verify and audit the ability to run and sustain production operations for a long period.

In this option, we don’t test DR runbooks, as this would imply the emergency restart, which has an impact on the production environment.

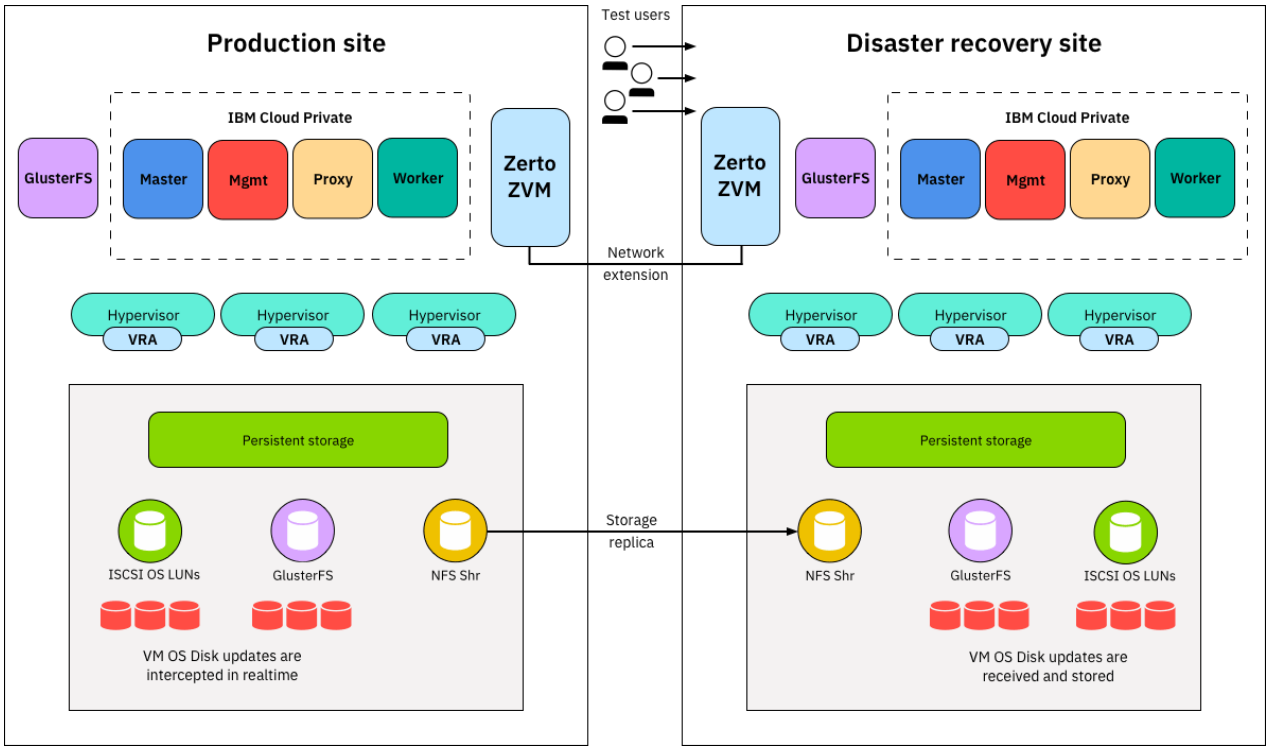
In the following diagram, you can see the technology-driven approach in the components of the IBM Cloud Private platform:



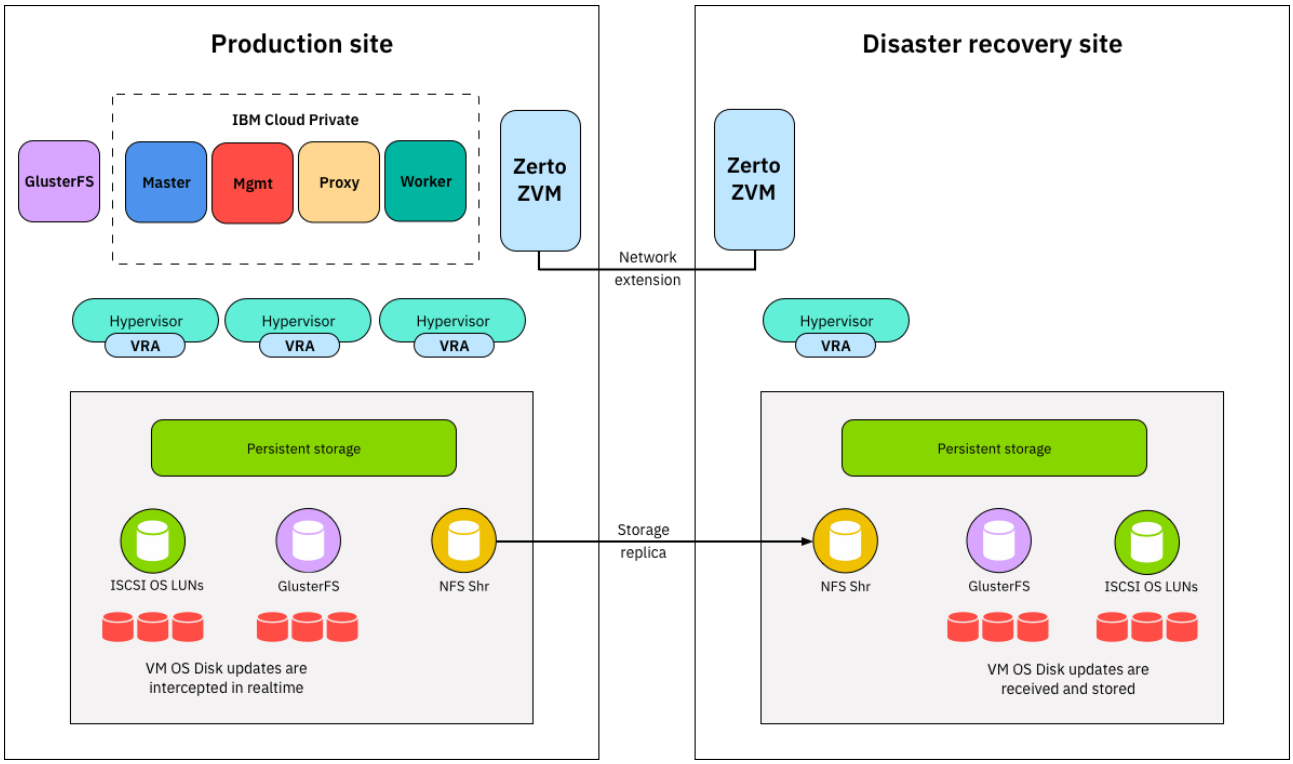
This diagram shows the status of the solution components after all of the subphases of the protection phase are completed.



This diagram shows the status of the solution components in the DR test stage:



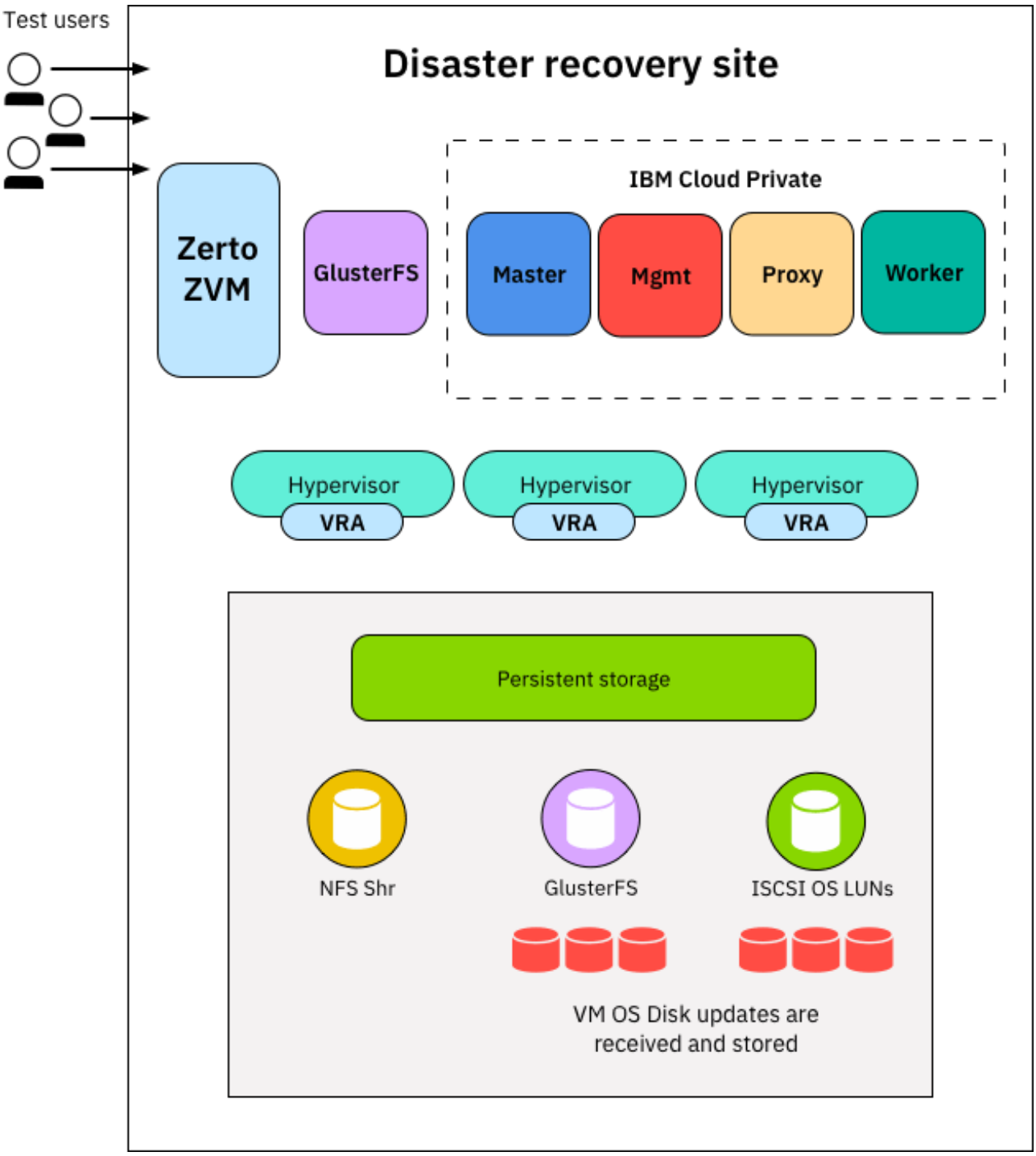
After these steps, your DR solution is back in the normal protection operation state.



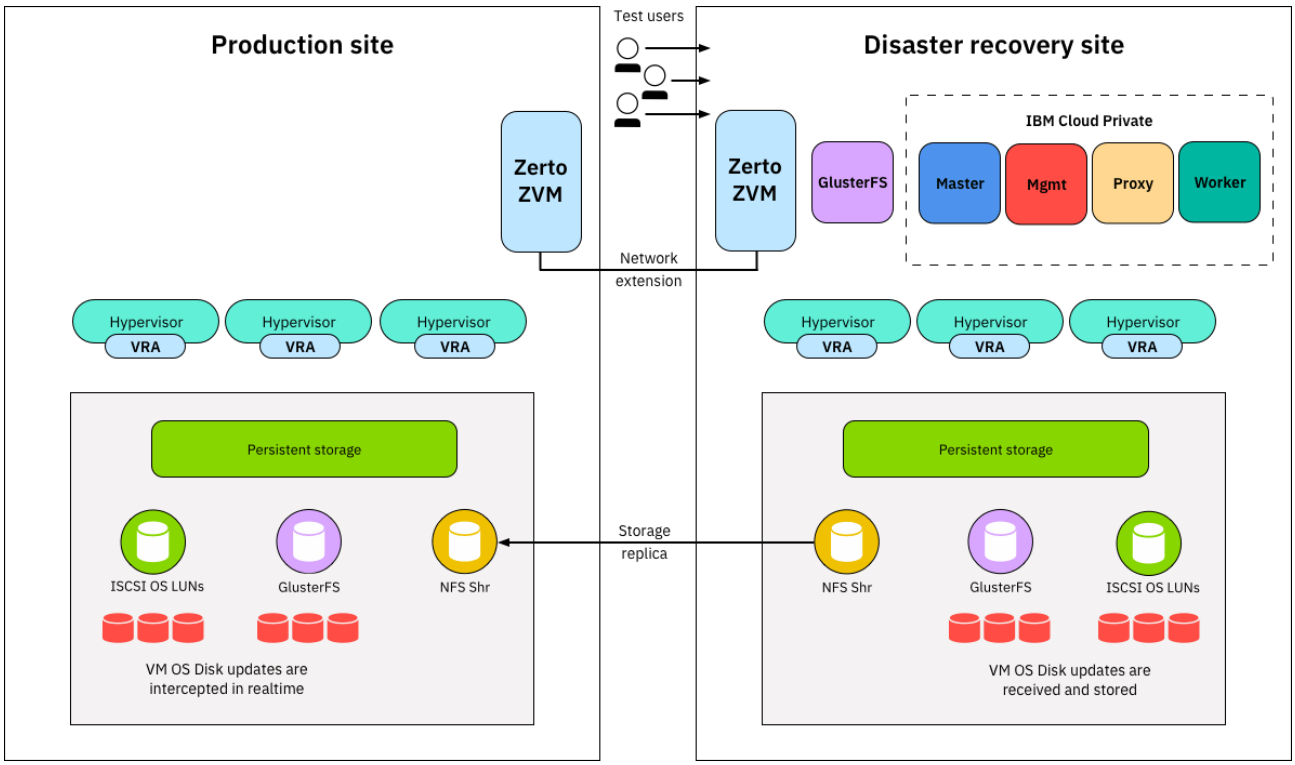
Emergency phase:

In an emergency, you complete the same operations in the DR test phase on disk.

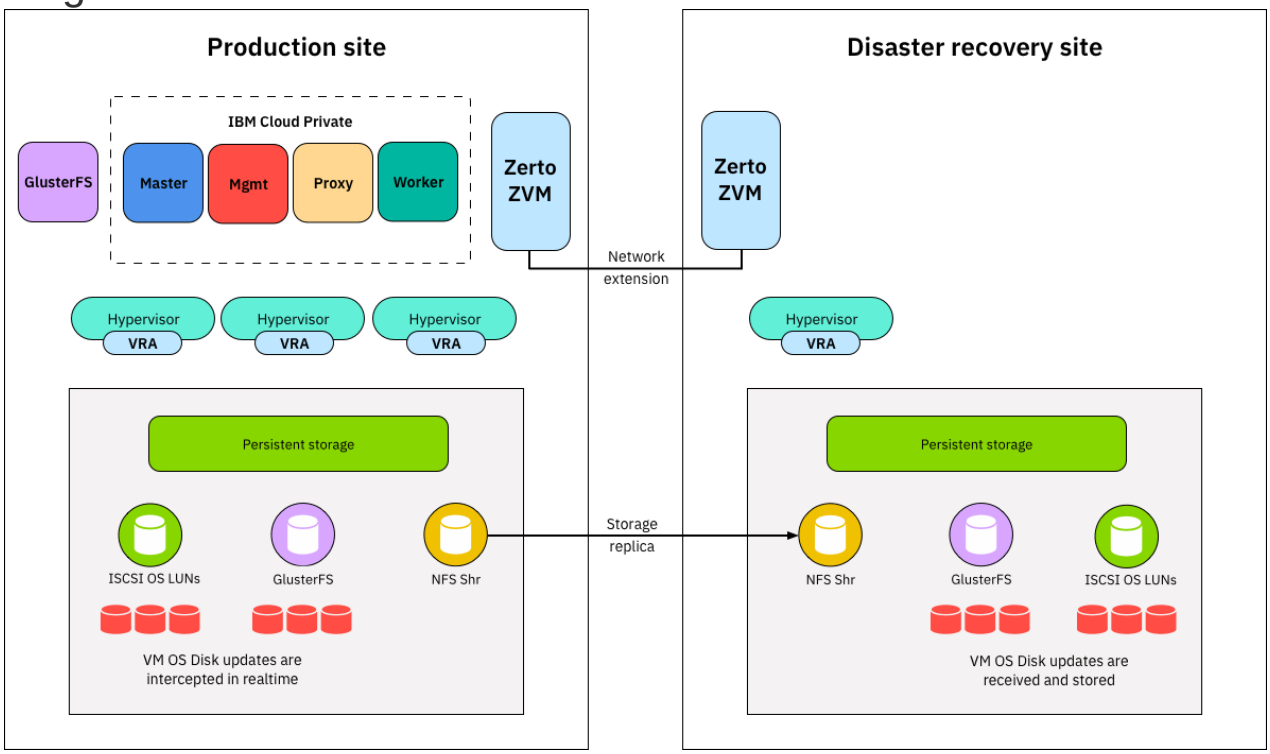
This diagram shows the status of the solution components in the emergency phase:



This diagram shows the status of the solution components at this stage:



This diagram shows the status of the solution components at this stage:



Testing disaster recovery:

Test disaster recovery implementation to validate the implementation and regularly test failover to your workload's DR Region to ensure that RTO and RPO are met.

A pattern to avoid is developing recovery paths that are rarely executed. For example, you might have a secondary data store that is used for read-only queries. When you write to a data store and the primary fails, you might want to fail over to the secondary data store. If you don't frequently test this failover, you might find that your assumptions about the capabilities of the secondary data store are incorrect. The capacity of the secondary, which might have been sufficient when you last tested, might no longer be able to tolerate the load under this scenario, or service quotas in the secondary Region might not be sufficient.

Our experience has shown that the only error recovery that works is the path you test frequently. This is the reason why having a small number of recovery paths is best.

You can establish recovery patterns and regularly test them. If you have a complex or critical recovery path, you still need to regularly execute that failure in production to validate that the recovery path works.

Manage configuration drift at the DR Region. Ensure that your infrastructure, data, and configuration are as needed at the DR Region. For example, check that AMIs and service quotas are up- to-date.

Disaster scenario:

In this scenario, your production environment is on-premises, and your disaster recovery plan involves using Google Cloud as the recovery site.

This scenario takes advantage of some of the HA features available in Google Cloud; you don't have to initiate any failover steps, because they occur automatically in the event of a disaster. The internal load balancer ensures that even when a replacement instance is needed, the same IP address is used for the database server. The instance template and custom image ensure that the replacement instance is configured identically to the instance it is replacing. By taking regular snapshots of the persistent disks, you ensure that when disks are re-created from the snapshots and attached to the replacement instance, the replacement instance is using data recovered according to an RPO value dictated by the frequency of the snapshots. In this architecture, the latest transaction log files that were written to the persistent disk are also automatically restored.

The managed instance group provides HA in depth. It provides mechanisms to react to failures at the application or instance level, and you don't have to manually intervene if any of those scenarios occur. Setting a target size of one ensures you only ever have one active instance that runs in the managed instance group and serves traffic.

Disaster practice:

t’s increasingly common for companies in all sectors to use the cloud to store their data. The cloud provides scalability, security and flexibility that was often inaccessible to businesses only a few years ago. But just like any other technology, it has its limits.

What happens if a severe thunderstorm knocks out power to a data center or if an employee accidentally deletes critical files? These are the types of scenarios that, however unlikely, can still happen and cause significant disruptions to a company if they’re not prepared.

That’s where cloud disaster recovery comes in. In this article, we’ll discuss why cloud disaster recovery is critical for businesses and the different strategies you can implement to ensure your date is always safe and accessible.